UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/895,498	06/29/2001	James S. Magdych	NAI1P012/01.132.01	8154

28875 7590 06/14/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
SHIFERAW, ELENI A	
ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 06/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/895,498	**Applicant(s)** MAGDYCH ET AL.	
	Examiner Eleni A. Shiferaw	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 March 2005*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *6/29/01* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

Final Rejection

Response to the applicant's amendments

1. Applicant's arguments/amendments with respect to amended claims 1, 18, and 36-38, and original claims 2-17, 19-35, and 39 filed March 30, 2005 have been fully considered but they are not persuasive. The examiner would like to point out that this action is made final (MPEP 706.07a).

Rejections

2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior office action.

Claim Rejections - 35 USC § 103

3. Claims 1-4, 18-22, 36, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. (Shostack, Patent No.: US 6,298,445 B1) in view of Fujimori (Patent No.: 6,681,212 B2).

As per claims 1, 18, and 36, Shostack teaches a method/system for detecting modifications to risk assessment scanning, comprising

(a) initiating a risk assessment scan on a target from a remote source utilizing a network (Shostack Col. 3 lines 15-17; the remote source module initiating risk assessment on the remote (target) computer connected to the network);

(c) receiving results of the risk assessment scan from the target utilizing the network (Shostack Col. 6 lines 67-col. 7 lines 4 and col. 3 lines 30-32; receiving risk assessment scan result from target computer utilizing the network); and

(d) notifying an administrator if any additional operations are carried out to improve a risk assessment in view of intrusion detection (Shostack Col. 6 lines 53-56; sending an alarm to the system administrator if risk assessment scan detects an intrusion is detection);

Shostack does not teach determining whether the risk assessment scan on the target involves an intermediate device coupled between the target and remote source. However Fujimori discloses

(b) detecting an intermediate device coupled between the target and the remote source (Fujimori Col. 2 lines 1-9; detecting an unauthorized node coupled between the authorized node and the monitor node).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Fujimori within the system of Shostack because it would avoid an authorized access by notifying (instructing) the user to use the protected mode (Fig. 4B No. 47, and col. 1 lines 62-67).

As per claim 2 and 19, Shostack and Fujimori teach all the subject matter as described above. In addition Fujimori teaches the method or a computer program product, wherein the intermediate device includes a router (Fujimori Col. 2 lines 1-9; detecting an unauthorized node (router) coupled between the authorized node and the monitor node).

As per claim 39 and 20, Shostack and Fujimori teach all the subject matter as described above. In addition Fujimori teaches the method or a computer program product, wherein the intermediate device includes a proxy server (Fujimori Col. 2 lines 1-9; detecting an unauthorized node (proxy server) coupled between the authorized node and the monitor node). The rational for combining are the same as claim 1 above.

As per claim 3 and 21, Shostack and Fujimori teach all the subject matter as described above. In addition Fujimori teaches the method or a computer program product, wherein a plurality of procedures are utilized to determine whether the risk assessment scan involves the intermediate device (Fujimori Col. 2 lines 1-9; detecting an unauthorized node coupled between the authorized node and the monitor node). The rational for combining are the same as claim 1 above.

As per claim 4 and 22, Shostack and Fujimori teach all the subject matter as described above. In addition Shostack teaches the method or a computer program product,
wherein at least one of the procedures includes determining a port list associated
with the risk assessment scan (Shostack Col. 7 lines 17-19).

As per claim 8 and 26, Shostack and Fujimori teach all the subject matter as described above. In addition Fujimori teaches the method or a computer program product,
wherein the communications include connection attempts between the remote

source and the target utilizing the network (Fujimori Col. 1 lines 36-40). The rational for combining are the same as claim 1 above.

As per claim 13 and 31, Shostack and Fujimori teach all the subject matter as described above. In addition Fujimori teaches the method or a computer program product, wherein the at least one of the procedures further includes indicating that the risk assessment scan involves the intermediate device based on the analysis (Fujimori Col. 2 lines 1-9; detecting an unauthorized node coupled between the authorized node and the monitor node). The rational for combining are the same as claim 1 above.

4. Claims 5-9, 23-27, and 37-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. (Shostack, Patent No.: US 6,298,445 B1) in view of Fujimori (Patent No.: 6,681,212 B2) and Applicant Admitted Prior Art (AAPA).

As per claim 37, and 38, Shostack teaches a method/computer program product for detecting modifications to risk assessment scanning caused by a proxy server, comprising:

(a) initiating a risk assessment scan on a target from a remote source utilizing a network (Shostack Col. 3 lines 15-17; the remote source module initiating risk assessment on the remote (target) computer connected to the network);

(d) receiving results of the risk assessment scan from the target utilizing the network (Shostack Col. 6 lines 67-col. 7 lines 4 and col. 3 lines 30-32; receiving risk assessment scan result from target computer utilizing the network);

(e) flagging the results of the risk assessment scan (Shostack Col. 6 lines 53-56; sending an alarm flag if risk assessment scan detects an intrusion is detection); and

(f) notifying an administrator if the results of the risk assessment scan on the target is flagged (Shostack Col. 6 lines 53-56; sending an alarm to the system administrator).

Shostack does not explicitly teach:

(b) executing a plurality of procedures to determine whether the risk assessment scan on the target involves a proxy server coupled between the target and the remote source;

However Fujimori discloses

executing a plurality of procedures to determine whether the risk assessment scan involves a proxy server coupled between the target and the remote source (Fujimori Col. 2 lines 1-9; detecting an unauthorized node coupled between the authorized node and the monitor node);

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Fujimori within the system of Shostack because it would avoid an authorized access by notifying (instructing) the user to use the protected mode (Fig. 4B No. 47, and col. 1 lines 62-67).

Shostack and Fujimori do not explicitly teach an ip_ttl flag, a tcp_win flag, a via tag, and a host header value.

However AAPA discloses ip_ttl flag, and tcp_win flag as a well known (AAPA page 6 par. 4-page 10 par. 2).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of AAPA within the combination system of Shostack and Fujimori because it would allow to determine unauthorized (intermediate) device by comparing the values of the flags. Data is sent to different nodes and tag values are compared. If the tag values are different identify the new node.

As per claim 5 and 23, Shostack, Fujimori, and AAPA teach all the subject matter as described above. In addition AAPA teaches the method/computer program product,
wherein the at least one of the procedures further includes ip_ttl flag, and tcp_win flag as a well known (AAPA page 6 par. 4-page 10 par. 2). The rational for combining are the same as claim 37 above.

As per claim 6 and 24, Shostack, Fujimori, and AAPA teach all the subject matter as described above. In addition AAPA teaches the method or a computer program product,
wherein the flag includes an ip-ttl flag as a well known (AAPA page 6 par. 4-page 10 par. 2). The rational for combining are the same as claim 37 above.

As per claim 7 and 25, Shostack, Fujimori, and AAPA teach all the subject matter as described above. In addition AAPA teaches the method or a computer program product, wherein the flag includes a tcp-win flag as a well known (AAPA page 6 par. 4-page 10 par. 2). The rational for combining are the same as claim 37 above.

As per claim 9 and 27, Shostack, Fujimori, and AAPA teach all the subject matter as described above. In addition AAPA teaches the method or a computer program product,
wherein the at least one of the procedures further includes indicating that the risk assessment scan involves the intermediate device, if the value of the flag is different for the communication attempts using the at least two ports on the port list (AAPA page 6 par. 4-page 10 par. 2; ip-ttl flag as a well known). The rational for combining are the same as claim 37 above.

5. Claims 10-14, and 28-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. (Shostack, Patent No.: US 6,298,445 B1) in view of Fujimori (Patent No.: 6,681,212 B2), and Mizrachi et al. (Mizrachi, Pub. No.: US 2003/0033486 A1).

As per claim 10 and 28, Shostack and Fujimori teach all the subject matter as described above.

Shostack and Fujimori do not explicitly teach transmitting request and cached version of the content to the target.

However Mizrachi discloses the method or a computer program product, wherein at least one of the procedures includes transmitting a first request for content to the target utilizing the network, and transmitting a second request for a cached version of the content to the target utilizing the network (Mizrachi Page 3 par. 0029).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings Mizrachi within the combination system of Shostack and Fujimori because the cache server would store cached content and identify the next user's access request from the cached content stored in the cache content server by comparing the newly access request and previously stored cached content and allow fast access if the newly access request is previously stored in the cache content server. It would be obvious to one skilled in the art to modify the teachings of Mizrachi and detect the new node by comparing cached content when cached content is different from target node.

As per claim 11 and 29, Shostack, Fujimori and Mizrachi teach all the subject matter as described above. In addition Mizrachi teaches the method or a computer program product, wherein the cached content is requested from the target utilizing a via tag (Mizrachi Page 1 par. 0033; TCP/IP Via tags is a well known TCP/IP tool for obtaining cached content utilizing the Internet). The rational for combining are the same as claim 10 above.

As per claim 12 and 30, Shostack, Fujimori and Mizrachi teach all the subject matter as described above. In addition Mizrachi teaches the method or a computer program product, wherein the at least one of the procedures further includes analyzing responses to the first and second requests (Mizrachi Page 3 par. 0029; analyzing access request and cached content). The rational for combining are the same as claim 10 above.

As per claim 14 and 32, Shostack, Fujimori and Mizrachi teach all the subject matter as described above. In addition, the method or a computer program product, wherein the at least one of the procedures further includes indicating that the risk assessment scan involves the intermediate device if the responses to the requests are different (Mizrachi Page 3 par. 0029, and Fujimori Col. 2 lines 1-9). The rational for combining are the same as claim 10 above.

Claims 15-17 and 33-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. (Shostack, Patent No.: US 6,298,445 B1) in view of Fujimori (Patent No.: 6,681,212 B2), and in further view of Hopmann et al. (Hopmann, Patent No.: US 6,578,069 B1).

As per claim 15 and 33, Shostack and Fujimori teach all the subject matter as described above.

Shostack and Fujimori so not explicitly teach request without specifying a host header value.

However Hopmann discloses the method/computer program product, wherein at least one of the procedures includes transmitting a request without specifying a host header value (Hopmann Col. 16 lines 6-11).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings Hopmann within the combination system of Shostack and Fujimori because it would create reconnection to the client.

As per claim 16 and 34, Shostack, Fujimori and Mizrachi teach all the subject matter as described above. In addition Hopmann teaches the method or a computer program product, wherein the at least one of the procedures further includes identifying an error message in response to the request (Hopmann Col. 16 lines 6-11).

As per claim 17 and 35, Shostack, Fujimori and Mizrachi teach all the subject matter as described above. In addition Hopmann teaches the method or a computer program product, wherein the at least one of the procedures includes indicating that the risk assessment scan involves the intermediate device, (Hopmann Col. 16 lines 6-11).

Response to the applicant's arguments

6. Applicant argues that:

a. Fujimori simply does not meet applicant's claimed "determining whether the risk assessment scan involves an intermediate device coupled between the target and the remote source." (page 10 par. 4)

b. Fujimori's authorized node and monitor node do not meet applicant's claimed target and remote source, as the authorized node is not the target of the risk assessment scan in Fujimori. (page 10 par. 5)

c. Prior art of record Shostack "sending an alarm to system administrator if an intrusion is detected" does not teach the claimed limitation as "notifying an administrator if it is determined that the risk assessment scan involves the intermediate device" There is no suggestion in Shostack of any sort of determination as to whether a risk assessment scan involves an intermediate device. (page 11 par. 4)

d. Prior art records do not teach, "Wherein additional operations are carried out to improve a risk assessment in view of the presence of the intermediate device.coupled between the target and the remote source." (page 11 par. 5)

e. At least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations. (page 12 par. 2)

f. Fujimori fails to teach, "A plurality of procedures are utilized to determine whether the risk assessment scan involves the intermediate device." (page 12 par. 3)

g. Shostack does not teach, "Wherein at least one of the procedures includes determining a port list associated with the risk assessment scan." (page 12 par. 4)

h. Claims 37 and 38 should be allowable for, at least in part, the reasons set forth herein above with respect to the aforementioned independent claims, the present claim further distinguish Fujimori by requiring a "proxy server" instead of "intermediate server", and the following limitations of claim 38 are not met by the prior art references:

"executing a plurality of procedures to determine whether the risk assessment scan involves a proxy server coupled between the target and the remote source;"

"receiving results of the risk assessment scan from the target utilizing the network;" and

"notifying an administrator if the results of the risk assessment scan are flagged." (page 13 par. 4-5)

I. All of the independent claims and dependent claims are deemed allowable. (page 14 par. 2)

However, Examiner disagrees with applicant.

Regarding argument (a), examiner disagrees with applicant. The prior art record Fujimori teaches the monitor node, which is connected to the communication network, remotely detects when an unauthorized node is connected to the network to make unauthorized copying (col. 2 lines 5-12).

Regarding argument (b), examiner disagrees with applicant. Fujimori's monitor node assesses the risk of unauthorized copying of data by an unauthorized node targeting the authorized node (col. 2 lines 5-12). Therefore, authorized node and monitor node do meet applicant's claimed target and remote source. Moreover, Fujimori discloses carrying out additional operations based on the presence of an unauthorized device "when unauthorized node is detected, monitor node instructs the target/authorized nodes to only perform in secure mode to avoid an unauthorized copying" (col. 2 lines 5-12).

Regarding argument (c), examiner disagrees with applicant. Shostack teaches notifying/alarming an administrator if intrusion is detected (col. 6 lines 53-56). Examiner stated on the office action page 3 lines 7-8 that Shostack does not teach an intermediate scan involves an intermediate device coupled between the target and remote device. Fujimori is cited for disclosing "detecting an unauthorized node coupled between the authorized node and monitor node" col. 2 lines 5-12. The office did not cite Shostack for alarming when intermediate device is detected. Sufficient motivation is provided to combine the teachings of Fujimori within Shostack on the office action page 3 lines 13-16.

Regarding argument (d), examiner disagrees with applicant. Fujimori discloses instructing the authorized nodes to use a protect/secure mode when unauthorized node is detected to improve the risk assessment (col. 2 lines 5-14).

Regarding argument (e), examiner disagrees with applicant. Prior art of record Shostack and Fujimori in combination teach all the limitations and sufficient motivation is provided.

Regarding argument (f), examiner disagrees with applicant. Fujimori teaches the first procedure performed on the monitor node on (fig. 3) and the other procedure is performed on authorized nodes on fig. 4B to determine whether the risk assessment scan involves an unauthorized node (page col. 2 lines 1-9).

Regarding argument (g), examiner disagrees with applicant. Shostack teaches continuous monitoring of the complete network, monitoring Internet Protocol devices, detecting potential security vulnerabilities, *providing a map of all ports on the network and* ***pings*** *(Packet Internet Groper is a basic Internet program that lets us verify that a particular address exists)* all Internet Protocol devices to expose potential security vulnerabilities (col. 7 lines 5-19).

Regarding argument (h), examiner disagrees with applicant. Based on the arguments set forth by the examiner for arguments (a)-(g), the independent claims 37 and 38 stand rejected. Fujimori's an unauthorized node could be a proxy server or intermediate server.

"executing a plurality of procedures to determine whether the risk assessment scan involves a proxy server coupled between the target and the remote source;" (see argument (f)) "receiving results of the risk assessment scan from the target utilizing the network;" (Shostack Col. 6 lines 67-col. 7 lines 4 and col. 3 lines 30-32; receiving risk assessment scan result from target computer utilizing the network); and

"notifying an administrator if the results of the risk assessment scan are flagged." (see argument (c))

Regarding argument (I), examiner disagrees with applicant. Based on the arguments set forth by the examiner for arguments (a) – (h), the dependent claims stand as rejected.

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw
June 8, 2005

E. Moise
EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER